The new WPA3 WiFi standard was officially released

On June 25, 2018, WiFi Alliance - the WiFi technology management organization announced the official release of WPA3. This is the latest WPA (WiFi Protected Access) standard, user authentication technology for WiFi connections.

On June 25, 2018, WiFi Alliance - the WiFi technology management organization announced the official release of WPA3. This is the latest WPA (WiFi Protected Access) standard, user authentication technology for WiFi connections.

News about the WiFi Alliance is preparing for a new standard that has been revealed since January. The organization began working on the new standard after a cyber security researcher revealed KRACK - a flaw in WiFi WPA2 security protocol that could allow an attacker to access the WPA2-protected WiFi transmission process. guard.

WPA3 is currently an option for new devices but it will work on all devices that meet this standard in the coming years. Specific dates have not been revealed, but WPA3 will keep the ability to interact with old WPA2 devices to ensure that the transition to WPA3 is not overlapped.

WPA3-Personal and WPA3-Enterprise

Like WPA1 and WPA2, WPA3 also has Personal and Enterprise security modes, the main difference being in the authentication stage. WPA3 uses SAE (Simultaneous Authentication of Equals) algorithm instead of PSK (Preshared Key) on WPA2-Personal, while WPA3-Enteprise has more advanced features instead of IEEE 802.1X from WPA2-Enterprise, including:

1. Authenticated encryption: 256-bit Galois / Counter Mode Protocol (GCMP-256)
2. Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
3. Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) uses 384-bit Elliptic curves
4. Robust management frame protection: 256-bit Broadcast / Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

WPA3 replaces the 14-year-old WPA2 standard

Enterprise mode encourages use in businesses, governments, and financial networks. Personal is the standard most normal people will use.

WPA3 against dictionary attacks

The WiFi Alliance said that WPA3's SAE will restrict offline dictionary attacks when an attacker tries to guess the WiFi password by trying several times. Security experts say that WPA3 will block authentication requests after several attempts, thereby limiting the effect of false testing.

SAE of WPA3 also uses forward secrecy name encryption, the key exchange authentication protocol where keys in the session work independently and is not lost even if the server is locked. has been revealed. This helps an attacker who gets a WiFi password also cannot decrypt the old traffic sent in the network by other members.

WiFi Easy Connect for WPA2 and WPA 3

Another WiFi feature is also announced with WPA3, which is WiFi Easy Connect, towards smart devices (IoT) without a screen to change WiFi network configuration. For example, you can use your phone / tablet to configure WiFi WPA3 for other devices.

WiFi Allian says WiFi Easy Connect will be available on devices running both WPA2 and WPA3, not only on WPA3.

Enhanced Open WiFi

Earlier this month, the WiFi Alliance also announced the release of WiFi Enhanced Open, proprietary technology that is only deployed on open WiFi networks such as airports and cafes. This technology uses OWE (Opportunistic Wireless Encryption) algorithm to encrypt each Connection between WiFi users and access points / routers with their own customized encryption key.

Encryption for each user helps an attacker not be able to peek at user traffic even if the network has no password.

See more:

1. What is WPA3 and when will you have it on your Wi-Fi?
2. What is the newly announced WPA3 WiFi security protocol?
3. KRACK attack breaks down the WPA2 WiFi protocol

You finished reading the article "**The new WPA3 WiFi standard was officially released**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
